UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/448,154	11/24/1999	PAUL S. GERMSCHEID	33012/274/10	4721

7590   12/31/2002

CHARLES A JOHNSON
UNISYS CORPORATION
LAW DEPARTMENT M S 4773
2470 HIGHCREST ROAD
ROSEVILLE, MN   55113

EXAMINER
WASSUM, LUKE S

ART UNIT	PAPER NUMBER
2177	

DATE MAILED: 12/31/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 07-01)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _04 November 2002_ .

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under _Ex parte Quayle_, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-20_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-20_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____ .

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)   4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)   5) ☐ Notice of Informal Patent Application (PTO-152)

3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .   6) ☐ Other: .

DETAILED ACTION

Response to Amendment

1.   An Applicants' amendment, filed 4 November 2002, has been received, entered into the

record, and considered.

2.   As a result of the amendment, claims 1-3, 6, 8, 11 and 12 have been amended. Claims 1-20

are now presented for examination.

Embodiment of the Invention

3.   The instant invention is a data processing system containing site-specific security profiles,

such that the user is allowed to access a database only from a specific terminal or location.

Claim Rejections - 35 *USC § 103*

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section
> 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the
> subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary
> skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the
> invention was made.

5.   This application currently names joint inventors. In considering patentability of the claims

under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was

commonly owned at the time any inventions covered therein were made absent any evidence to the

contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and

invention dates of each claim that was not commonly owned at the time a later invention was made

in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35

U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

6.   Claims 1-4, 6-8, 11-14 and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable

over **Garrison** (U.S. Patent 6,275,939) in view of **Yoshimoto** (U.S. Patent 6,237,023).

7.   Regarding claim 1, **Garrison** teaches a data processing environment having a user terminal at

a site for generating a service request responsively coupled via a publicly accessible digital data

communication network to a database management system having at least one database as claimed,

comprising security profile corresponding to a site whereby said database management system

permits said user terminal to access said at least one database (see col. 4, lines 1-32; see also col. 6,

line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

        Garrison does not explicitly teach a data processing environment wherein the security

profile is site-specific.

        Yoshimoto, however, teaches a data processing environment wherein the security profile is

site-specific (see Abstract; see also col. 1, line 63 through col. 2, line 6).

        It would have been obvious to one of ordinary skill in the art at the time of the invention to

incorporate a site-specific security profile, since this would allow the level of access granted to a user

to be based in part on the security of the specific terminal or location from which the access request

is generated, thus inhibiting illegitimate access from a terminal having poor security (see col. 6, lines 15-21).

8.   Regarding claim 6, **Garrison** teaches an apparatus as claimed, comprising:

a) a user terminal located at a site (see col. 4, lines 1-32);

b) a database management system having access to a database responsively coupled to said user terminal via a publicly accessible digital data communication network (see col. 4, lines 1-32); and

c) a security profile generated by said database management system corresponding to said site whereby said database management system provides access to a particular portion of said database corresponding to said security profile (see col. 7, line 50 through col. 8, line 37).

Garrison does not explicitly teach a data processing environment wherein the security profile is site-specific.

Yoshimoto, however, teaches a data processing environment wherein the security profile is site-specific (see Abstract; see also col. 1, line 63 through col. 2, line 6).

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a site-specific security profile, since this would allow the level of access granted to a user to be based in part on the security of the specific terminal or location from which the access request

is generated, thus inhibiting illegitimate access from a terminal having poor security (see col. 6, lines 15-21).

9.   Regarding claim 11, **Garrison** teaches a method of utilizing a user terminal located at a site to access a remote database management system having a database via a publicly accessible digital data communication network as claimed, comprising:

> a) transmitting a service request requiring access to said database from said user terminal (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37);

> b) receiving said service request by said remote database management system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37);

> c) determining a security profile corresponding to said site (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37);

> d) comparing said security profile with said service request (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37); and

> e) honoring said service request if and only if said service request corresponds to said security profile (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

Garrison does not explicitly teach a data processing environment wherein the security profile is site-specific.

Yoshimoto, however, teaches a data processing environment wherein the security profile is site-specific (see Abstract; see also col. 1, line 63 through col. 2, line 6).

It would have been obvious to one of ordinary skill in the art at the time of the invention to

incorporate a site-specific security profile, since this would allow the level of access granted to a user

to be based in part on the security of the specific terminal or location from which the access request

is generated, thus inhibiting illegitimate access from a terminal having poor security (see col. 6, lines

15-21).

10.   Regarding claim 16, **Garrison** teaches an apparatus as claimed, comprising:

a) means located at a site for permitting a user to interact with a database responsively

coupled via a publicly accessible digital data communication network (see col. 4, lines

1-32);

b) means responsively coupled to said permitting means via said publicly accessible digital

data communication network for offering data processing services involving access to

said database in response to said service request (see col. 6, line 60 through col. 7, line

32; see also col. 7, line 50 through col. 8, line 37); and

c) means responsively coupled to said offering means for preventing said offering means

from offering said data processing services to said user in response to said service

request unless said site corresponds to a security profile wherein said security profile

permits access to said database (see col. 6, line 60 through col. 7, line 32; see also col.

7, line 50 through col. 8, line 37).

Garrison does not explicitly teach a data processing environment wherein the security

profile is site-specific.

Yoshimoto, however, teaches a data processing environment wherein the security profile is site-specific (see Abstract; see also col. 1, line 63 through col. 2, line 6).

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a site-specific security profile, since this would allow the level of access granted to a user to be based in part on the security of the specific terminal or location from which the access request is generated, thus inhibiting illegitimate access from a terminal having poor security (see col. 6, lines 15-21).

11.   Regarding claim 2, Garrison additionally teaches an improvement wherein said security profile is generated by said data management system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

12.   Regarding claims 3, 8, 12, 13 and 18, Garrison additionally teaches an improvement, method and apparatus further comprising a special field responsively coupled to a service request whereby said database management system receives said special field and generates said security profile corresponding to said site and to said special field (see discussion of predefined password at col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

13.   Regarding claims 4, 14 and 17, Garrison additionally teaches an improvement, method and apparatus wherein said publicly accessible digital data communication network further comprises the Internet (see col. 4, lines 1-32).

14.   Regarding claim 7, **Garrison** additionally teaches an apparatus wherein said user terminal

accesses said data entity by transferring a service request to said system (see col. 6, line 60 through

col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

15.   Claims 5, 9, 10, 15, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Garrison (U.S. Patent 6,275,939) in view of **Yoshimoto** (U.S. Patent 6,237,023) as applied to claims

1-4, 6-8, 11-14 and 16-18 above, and further in view of **King** ("Hazards Control Department Use of

the Sperry Database Management System MAPPER").

16.   Regarding claims 5, 9, 15 and 19, **Garrison** teaches an improvement to a data processing

environment, method and apparatus substantially as claimed.

        Garrison does not teach the improvement, method and apparatus wherein said database

management system is MAPPER.

        However, **King** teaches a system wherein the database management system used is

MAPPER (see first paragraph).

        It would have been obvious to one of ordinary skill in the art at the time of the invention to

use MAPPER as the database management system, since MAPPER is extremely versatile and is

considered one of the best fourth generation programs, and furthermore since it contains, in

addition to a database management system, a word processor, office automation program including electronic mail, and color graphics routines (see first paragraph).

17.   Regarding claim 10, **Garrison** additionally teaches an apparatus wherein said publicly accessible digital data communication network further comprises the World Wide Web (see col. 4, lines 1-32).

18.   Regarding claim 20, **Garrison** additionally teaches an apparatus wherein said permitting means further comprises an industry standard personal computer (see col. 4, lines 1-60).

19.   Claims 5, 9, 10, 15, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garrison** (U.S. Patent 6,275,939) in view of **Yoshimoto** (U.S. Patent 6,237,023) as applied to claims 1-4, 6-8, 11-14 and 16-18 above, and further in view of **Unisys** ("Why Do I Need Cool ICE?").

20.   Regarding claims 5, 9, 15 and 19, **Garrison** teaches an improvement to a data processing environment, method and apparatus substantially as claimed.

        Garrison does not teach the improvement, method and apparatus wherein said database management system is MAPPER.

        However, **Unisys** teaches a system wherein the database management system used is MAPPER (see page 3, second paragraph).

It would have been obvious to one of ordinary skill in the art at the time of the invention to
use MAPPER as the database management system, since MAPPER has been tuned for reliability,
scalability, and high performance, and furthermore, since the technology has been used for years by
thousands of users for many different kinds of applications, and since it has gained a reputation for
performing well for everything from small data analysis applications to huge transaction systems,
and since its reliability is exemplary (see page 3, second paragraph).

21.   Regarding claim 10, **Garrison** additionally teaches an apparatus wherein said publicly
accessible digital data communication network further comprises the World Wide Web (see col. 4,
lines 1-32).

22.   Regarding claim 20, **Garrison** additionally teaches an apparatus wherein said permitting
means further comprises an industry standard personal computer (see col. 4, lines 1-60).

23.   Claims 5, 9, 10, 15, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over
Garrison (U.S. Patent 6,275,939) in view of **Yoshimoto** (U.S. Patent 6,237,023) as applied to claims
1-4, 6-8, 11-14 and 16-18 above, and further in view of **Gebauer** (U.S. Patent 6,324,539).

24.   Regarding claims 5, 9, 15 and 19, **Garrison** teaches an improvement to a data processing
environment, method and apparatus substantially as claimed.

Garrison does not teach the improvement, method and apparatus wherein said database
management system is MAPPER.

However, **Gebauer** teaches a system wherein the database management system used is MAPPER (see col. 1, lines 56-65).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER is one of the most successful database management systems available (see col. 1, lines 56-65), and furthermore that providing access to a proprietary database management system such as MAPPER through the Internet would yield an extremely inexpensive and universally available means for accessing the data which it contains and such access would be without the need for considerable specialized training (see col. 2, lines 45-51).

25.   Regarding claim 10, **Garrison** additionally teaches an apparatus wherein said publicly accessible digital data communication network further comprises the World Wide Web (see col. 4, lines 1-32).

26.   Regarding claim 20, **Garrison** additionally teaches an apparatus wherein said permitting means further comprises an industry standard personal computer (see col. 4, lines 1-60).

Response to Arguments

27.   Applicant's arguments with respect to claims 1-20 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

28.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure.

       Foladare et al. (U.S. Patent 6,249,815) teaches a service optimizer for establishing an initial

subscriber profile, wherein access to a subscriber profile for the purposes of updating can be

contingent on the subscriber accessing the system from a specific terminal.

       Lerner et al. (U.S. Patent 6,157,722) teaches an encryption key management system and

method of securely communicating data, wherein access to a cell phone system is contingent upon

the physical location from which the request is made.

       Meyers et al. (U.S. Patent 5,937,159) teaches a method of controlling access of users to a

trusted computer system using an authentication and authorization database, including a credential

daemon for making decisions on user access based on username, service, location, and time.

       Faber (U.S. Patent 4,891,838) teaches a computer accessing system wherein access is granted

based on the password and specific terminal from which the access request has been received.

       Hale et al. (U.S. Patent 4,652,698) teaches a security method and system wherein, before a

user can access data from the central processor, the user's assigned terminal must first verify that the

user is the proper user of that terminal, and then the central processor must verify that the terminal

requesting the data is authorized to access that data.

       Levine (U.S. Patent 4,531,023) teaches a computer security system wherein a file is

maintained containing the telephone numbers of all authorized users, and access is allowed only for

those users providing the corresponding password while connected from a corresponding

authorized telephone number.

Smith (U.S. Patent 4,520,233) teaches a telephone security apparatus which prevents

completion of a connection to the terminal equipment unless the incoming call provides a

predefined access code and the call is found to have been made from the remote subscriber station

to which the predefined access code has been assigned.

Atalla (U.S. Patent 4,288,659) teaches an improved secured data transmission system which

relies on the favorable comparison of coded signals derived from information about authorized

individuals and particular data terminals that is both prestored and subsequently supplied under

manual command.

Any inquiry concerning this communication or earlier communications from the examiner

should be directed to Luke S. Wassum whose telephone number is 703-305-5706. The examiner can

normally be reached on Monday-Friday 8:30-5:30, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,

John E. Breene can be reached on 703-305-9790. The fax phone numbers for the organization

where this application or proceeding is assigned are 703-746-7239 for regular communications and
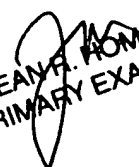
703-746-7238 for After Final communications.

In addition, INFORMAL or DRAFT communications may be faxed directly to the examiner

at 703-746-5658.

Any inquiry of a general nature or relating to the status of this application or proceeding

should be directed to the receptionist whose telephone number is 703-305-3900.

Luke S. Wassum
Art Unit 2177

lsw
December 24, 2002